修 士 学 位 論 文

論文題名

楕円曲線と Elliptic Divisibility Sequence 上における計算困難問題の関係性について

指導教員　内田 幸寛 准教授

2020 年 1 月 10 日 提出

首都大学東京大学院

理学研究科 数理科学専攻

学修番号 18843409

氏名 樺島 祐

目次

1 前文

今日では, 通信技術などの日常の様々な場面で暗号理論が用いられている. 情報の機密性の根幹にある暗号化で用いられる計算問題の困難性に関する理論は極めて重要である. そこで本論文では, 有名な計算困難問題の計算量の関係性について考察した.

$\mathbb{F}_q$ を位数 q の体とする (標数 $p \neq 2, 3$) . $\mathbb{F}_q$ 上の楕円曲線 E を

$$E : y^2 = x^3 + Ax + B$$

と定義する. ただし, $4A^3 + 27B^2 \neq 0$ であるとする. また, 楕円曲線 E 上の $\mathbb{F}_q$ 有理点のなす群 $E(\mathbb{F}_q)$ を

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 | y^2 = x^3 + Ax + B\} \cup \{O\}$$

とする. ここで, O は無限遠点を表す. また, $r \in \mathbb{Z}$ とし, $\mathbb{F}_q$ 上の r-ねじれ点の集合を

$$E_r = E(\mathbb{F}_q)[r] = \{P \in E(\mathbb{F}_q) | rP = O\}$$

で表す. 本論文では, $r > 3, \gcd(r, q-1) = 1$ となる r を固定しておく.

本論文の先行研究として, [4] や [10] で, 暗号理論に利用される計算困難問題の関係について述べられている. 本論文では, 上の条件を満たすような r を固定しておくことで, 楕円曲線上の位数が素数でない点におけるこれらの問題の関係を一般化することを考える.

簡単のため, 本論文においては上記 2 つの先行研究の論文と同様に, $\mathbb{F}_q$ 上の基本的な計算にかかる時間はすべて $O(\log^2 q)$ であるものとする. この条件のもとで, 本論文においては具体的に以下の 5 つの計算困難問題の関係性を考える.

問題 1. (Elliptic Curve Discrete Logarithm Problem (ECDLP))
$P \in E_r$ $(\mathrm{ord}(P) \geq 4), Q \in \langle P \rangle$ が与えられたとき, $Q = kP$ を満たす $k \in \mathbb{Z}$ を計算せよ.

問題 2. (EDS Association)
$P \in E_r, Q \in \langle P \rangle$ が与えられたとき, $Q = kP$ を満たす $k \in \mathbb{Z}$ について, $W_{E,P}(k)$ を計算せよ.

問題 3. (EDS Residue)
$P \in E_r, Q \in \langle P \rangle$ が与えられたとき, $Q = kP$ を満たす $k \in \mathbb{Z}$ について, $W_{E,P}(k)$ が $\mathbb{F}_q$上平方剰余か否か判定せよ.

問題 4. (Width s EDS Discrete Log)
$P \in E_r$ とする. $\phi(kP), \phi((k+1)P), \cdots, \phi((k+s-1)P)$ が与えられたとき, k を計算せよ.

問題 5. (EDS-Diffie Hellman (EDS-DH))
$P \in E_r$とする.$P, aP, bP (a, b \in \mathbb{Z})$ が与えられたとき, $\phi(abP)$ を計算せよ.

問題 6. (ECDHP)
$P \in E_r$とする.$P, aP, bP (a, b \in \mathbb{Z})$ が与えられたとき, abP を計算せよ.

各問題を記述するために必要な用語の定義については後に Section 2 で与えることにする. また, 問題 5 の ϕ は主結果 1 で定義している. これらの問題のいずれかが計算できるという仮定が与えられたとき, 他の問題

を解くためにかかる計算量について考察し, 以下の主結果 2 を得た. また, そのために必要な定理として, 主結果 1 を示した.

主結果 1. $P \in E_r$とする.

$$\phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+r)} \right)^{\frac{1}{r^2}} \tag{1}$$

と定義する. ただし, $\phi(O) = 0$ とする. このとき,

$$\phi(nP) = \phi(P)^{n^2} W_{E,P}(n) \tag{2}$$

が成り立つ. また, $\phi(nP)$ は EDS になる.

式 (1) は, [4] の Theorem 6 で定義されている $\phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+\mathrm{ord}(P))} \right)^{\frac{1}{\mathrm{ord}(P)^2}}$ の類似である. 本論文では r を固定しておくことで, 定義に $\mathrm{ord}(P)$ を用いず, これにより $P \in E_r,\ \gcd(r, q-1) = 1$ となる範囲では $\mathrm{ord}(P)$ が合成数である場合においても議論することができる. 本論文では, 楕円曲線上の位数が素数でない点においてこれらの問題の関係を一般化することを考え, 以下の主結果 2 を示した.

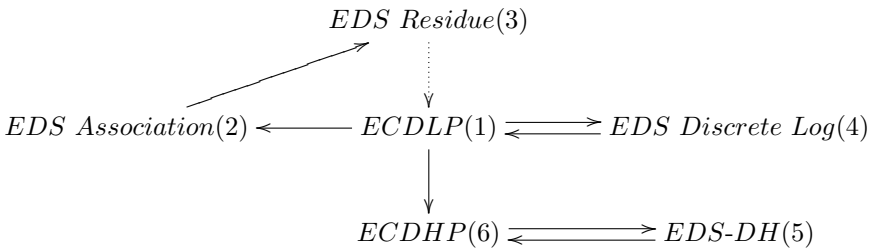
主結果 2. $\phi(P)$ が $\mathbb{F}_q$ 上の原始根であるとき, 以下が成り立つ.
問題 1, 問題 4 は, いずれか一方の問題にもう一方の問題を多項式時間で帰着できる. また, 問題 3 は問題 2 に, 問題 2 は問題 1 に多項式時間で帰着できる.
問題 5 と問題 6 はいずれか一方の問題をもう一方の問題に多項式時間で帰着でき, 問題 6 は問題 1 に多項式時間で帰着できる.
更に, 問題 3 が $O(T(q))$ で解けるならば, 問題 1 を $O(\log q(T(q) + \log^4 q))$ で 解くことができる. また, 問題 2 が解けるとき, 問題 1 を $\mathbb{F}_q$ 上の離散対数問題に帰着できる.

これらの証明は Section 3 で与える.

また, 主結果 2 から, 次の結論を導くことができる.

$\phi(P)$ が $\mathbb{F}_q$ 上の原始根であるとき, 問題 1, 問題 2, 問題 3, 問題 4 ($s = 3$) のいずれかが確率的準指数時間で解けるならば, 残る 3 つの問題も確率的準指数時間で解くことができる.
また, 問題 5, 問題 6 のいずれかが確率的準指数時間で解けるならば, もう一方の問題も確率的準指数時間で解くことができる. また, 問題 1 が確率的準指数時間で解けるとき, 問題 5, 問題 6 は確率的準指数時間で解くことができる.

まとめると, 下の図式のように多項式時間で行き来できることが示せた.



実線部分は多項式時間で計算できる. 破線部分 (問題 3 →問題 1) は主結果 2 のとおり.

問題 2 は体 $\mathbb{F}_q$ の標数が 2 でないときは, 問題 3 に帰着させてから問題 3 を問題 1 に帰着させることができるが, 標数が 2 であるときは問題 3 を考えることができない. 問題 2 を問題 3 を経由せずに問題 1 に帰着させるためには, 体 $\mathbb{F}_q$ 上の離散対数問題を解くことになる.

2 準備

まず, 主張に用いる基本的な用語の定義と基本的な性質を記述する.

定義 1. (EDS)

写像 $W : \mathbb{Z} \to \mathbb{F}_q$ が elliptic divisibility sequence (EDS) であるとは, 任意の $m, n \in \mathbb{Z}$ について, 以下の漸化式が成り立つことである.

$$W(m+n)W(m-n)W(1)^2 = W(m+1)W(m-1)W(n)^2 - W(n+1)W(n-1)W(m)^2. \tag{3}$$

本論文では, EDS を上のように 1 次元の elliptic net として定義する. EDS の漸化式から, 直ちに次の公式が得られる.

$m = n+1$, $n = n$ とすることで,

$$W(2n+1)W(1)^4 = W(n+2)W(n)^3 - W(n-1)W(n+1)^3. \tag{4}$$

また, $m = n+1$, $n = n-1$ とすることで,

$$W(2n)W(2)W(1)^2 = W(n)\left(W(n+2)W(n-1)^2 - W(n-2)W(n+1)^2\right). \tag{5}$$

更に, $W(1) \neq 0$ の条件下では,

$$W(-n) = -W(n)$$

が成り立つことが知られている.

定義 2. (等分多項式)

$n \in \mathbb{Z}$ とする. 次で定まる多項式 $\psi_n \in \mathbb{Z}[x, y, A, B]$ を等分多項式という.

$$\begin{aligned}
\psi_0 &= 0, \\
\psi_1 &= 1, \\
\psi_2 &= 2y, \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \ (n \geq 2), \\
\psi_{2n} &= (2y)^{-1}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \ (n \geq 3), \\
\psi_{-n} &= -\psi_n \ (n \leq 0).
\end{aligned}$$

命題 1. $P = (x, y) \in E(\mathbb{F}_q)$ とする. $W_{E,P}(n) = \psi_n(P)$ と定義すると, $W_{E,P} : \mathbb{Z} \to \mathbb{F}_q$ は EDS である.

証明は [9] の Section 9.5 を参照せよ. この命題により, 楕円曲線 $E(\mathbb{F}_q)$ とその曲線上の点 P が定まれば, 対応する EDS が定まることがわかる. したがって, 楕円曲線上の計算問題と EDS 上の計算問題を対応させることができる.

定理 1. 任意の $m, n \in \mathbb{Z}$ に対して,

$$W_{E,P}(mn) = W_{E,mP}(n) \cdot W_{E,P}(m)^{n^2}$$

が成り立つ.

この証明は等分多項式を Weierstrass の σ-関数で書き表し, 具体的に計算することで導くことができる. 詳細については [8] を参照せよ.

定義 3. (rank of zero-apparition)
W : EDS とする. $\rho \in \mathbb{Z}_{>0}$ が W の rank of zero-apparition であるとは, $W(\rho) = 0$ かつ, 任意の $0 < m < \rho$ に対して $W(m) \neq 0$ であることをいう.

[4] の Problem 4 では, 本論文の問題 4 （Width s EDS Discrete Log）を, W の rank of zero-apparition が素数である場合として定義している. 本論文では, この条件は外して考える.

次に, ここまでの定義と基本的な性質を使って, 本論文の主結果を導くために必要な主張を述べていく.

補題 1. $P \in E_r$ とする. 点 P の x 座標を $x(P)$ と表すことにする. $W_{E,P}(n-1), W_{E,P}(n), W_{E,P}(n+1)$ の 3 項, もしくは $\phi((n-1)P), \phi(nP), \phi((n+1)P)$ の 3 項が与えられたとき, nP の x 座標 $x(nP)$ は $O(\log^2 q)$ で計算することができる.

証明 . [7] の Lemma 6.2.2 より, 次の式を得る.

$$\frac{W_{E,P}(n-1)W_{E,P}(n+1)}{W_{E,P}(n)^2} = x(P) - x(nP). \tag{6}$$

今, $x(nP)$ 以外の項は全て仮定の下で $O(\log^2 q)$ で計算できるため, $x(nP)$ は $O(\log^2 q)$ で計算することができる. また, 式 (2) を用いることで, $\phi(nP)$ から $W_{E,P}(nP)$ を計算できる. □

定理 2. $t \in \mathbb{Z}$ が与えられたとき, $W_{E,P}(t)$ を $O(\log |t| \log^2 q)$ で計算することができる.

証明 . アルゴリズム ([5] Theorem 3.4.1) による. $W_{E,P}(k-3)$ から $W_{E,P}(k+4)$ までの連続した 8 個の項を $\langle W_{E,P}(k)\rangle$ と書き表すとする. $\langle W_{E,P}(t)\rangle$ は $\langle W_{E,P}(1)\rangle$ をもとに, (4), (5) を用いて繰り返し 2 倍算と加法を行うことによって求められる. まず, $\langle W_{E,P}(1)\rangle$ を計算しておく. これは, $W_{E,P}(0)=0, W_{E,P}(1)=1, W_{E,P}(-n)=-W(n)$ だから, $W_{E,P}(i)$ $(i=2,3,4)$ を EDS の漸化式を用いて計算すればよい.

1. $t=2^l\mu_0$ (μ_0 : 奇数) となる μ_0 を計算する.
2. $\mu_j=\lfloor\frac{\mu_{j-1}}{2}\rfloor$ として $\mu_1,\ \cdots,\ \mu_{m-1}=2$ or $3,\ \mu_m=1$ を計算する.
3. $j=m,\ \cdots,\ 1$ について, 次の計算を繰り返す.
   $\mu_{j-1}=2\mu_j$ のとき, $\langle W_{E,P}(2\mu_j)\rangle$ を計算する.
   $\mu_{j-1}=2\mu_j+1$ のとき, $\langle W_{E,P}(2\mu_j+1)\rangle$ を計算する.
   これにより, 最終的に $\langle W_{E,P}(\mu_0)\rangle$ を得る.
4. $\langle W_{E,P}(2\mu_0)\rangle, \langle W_{E,P}(2^2\mu_0)\rangle, \cdots, \langle W_{E,P}(2^l\mu_0)\rangle=\langle W_{E,P}(t)\rangle$ を計算する.

Step 3 及び Step 4 の計算には, 式 (4), (5) を用いる. これら計算は $O(\log^2 q)$ で $O(\log|t|)$ 回行われる. □

定理 3. $P\in E_r$ とする. $Q=kP$ が与えられたとき, $\phi(Q)$ を $O(\log^3 q)$ で計算できる.

証明 . 主結果 1 の式 (1) を考えると, 右辺の括弧内の計算にかかる時間は, 定理 2 より, $O(\log(q-1+r)\log^2 q)+O(\log(q-1)\log^2 q)+O(\log^2 q)=O(\log^3 q)$. このほかに行うのは $\mathbb{F}_q$ 上の指数の計算で, これは $O(\log q)$ で計算することができる. □

定理 4. $P\in E_r$ とする. $\phi(kP),\phi((k+1)P),\phi((k+2)P)$ が与えられたとき, $Q=kP$ を確率的に $O(\log^4 q)$ で計算することができる.

証明 . 補題 1 により, $x((k+1)P)$ は $O(\log^2 q)$ で計算される. また, 対応する 2 つの y 座標は, [2] Section 7.1 より, 確率的に $O(\log^4 q)$ で計算される. 2 つの $(k+1)P$ の候補から正しいものを選ぶには, まず, どちらかを $(k+1)P$ と仮定し, 楕円曲線上の加法により, $x((k+2)P)$ を計算する. そして, 補題 1 の式 (6) で $n=k+2$ として,

$$\frac{W_{E,P}(k+1)W_{E,P}(k+3)}{W_{E,P}(k+2)^2}=x(P)-x((k+2)P).$$

これを仮定のもとで解いて, $\phi((k+3)P)$ を決定する. これと同様に $\phi((k+4)P)$ を決定し, EDS の漸化式で $m=k+2, n=2$ としたものが成り立った場合, 初めに仮定した $(k+1)P$ が正しいとわかる. そうでなければ, もう一方の候補が正しい $(k+1)P$ である. 以上により $(k+1)P$ が求まれば, $Q=kP=(k+1)P-P$ を計算することで Q が定まる. □

次の定理 5 を示すために, 本論文の主結果 1 を用いる.

定理 5. $P\in E_r$ とし, $\phi(P)$ が $\mathbb{F}_q$ の原始根であるとする. k $(0\le k<\mathrm{ord}(P))$ について, $W_{E,P}(k), W_{E,P}(k+1), W_{E,P}(k+2)$ が与えられたとき, k を計算することは, 確率的に $O(\log^4 q)$ の計算で $\mathbb{F}_q$ 上の離散対数問題を解くことに帰着できる.

証明 . 補題 1 より, $x(Q)$ を計算し, 楕円曲線の式に代入することで対応する Q の候補を 2 つ求めると, [2] Section 7.1 より, これは確率的に $O(\log^4 q)$ で計算される. 求めた候補を $kP, -kP$ とする. 定理 4 と同様に

して Q を決定する. 主結果 1 の式 (2) より,

$$\frac{\phi((k+1)P)}{\phi(kP)} = \phi(P)^{2k+1}\frac{W_{E,P}(k+1)}{W_{E,P}(k)}$$

を得る. よって, $A = \frac{\phi((k+1)P)W_{E,P}(k)}{\phi(kP)W_{E,P}(k+1)}$, $B = \phi(P)$ とすれば, A, B はともに計算でき, 離散対数問題 $A = B^{2k+1}$ を解くことで $2k+1$ の値を得る. ただし, $\mathrm{ord}(P) < q-1$ のとき, k は 2 つの値をとる. □

命題 2. $P \in E_r, Q = kP$ とする. また, k の偶奇を $O(T(q))$ で計算する方法が既知であるとする. このとき, ECDLP を解いて k を $O(\log q(T(q) + \log^3 q))$ で計算できる.

証明 . 次の Step 1〜3 の手順による.

1. $Q = P$ ならば, $k = 1$ として終了.
2. 仮定により, k の偶奇を $O(T(q))$ で決定する. k が偶数ならば, $2Q' = Q$ となる Q' を計算する. k が奇数ならば, $2Q' = Q - P$ となる Q' を計算する.
3. $Q = Q'$ として, Step 1 に戻る.

Step 2 について, $\mathbb{F}_q$ の標数が 2 でなく, $\gcd(r, q-1) = 1$ であるから, r は奇数である. したがって, P, Q の位数は奇数であり, 特に, E_r に 2-ねじれ点は存在しない. ゆえに, Q' は一意に定まる. これにかかる時間は $Q - P$ と 2^{-1} の計算及び乗算で, $O(\log^3 q)$ である. 更に, $Q' = k'P$ とすると, 毎回の Step 2 において, k' が偶数であれば 0, 奇数であれば 1 を記録しておき, 終了後にこれらを右から並べることで k の二進数表記を得る. また, その回数は $\log_2 k = O(\log q)$ である. □

命題 3. $P \in E_r$, $Q = kP$ とする. また, $\phi(P)$ が平方非剰余であるとする. このとき, $e_i \in \mathbb{Z}, p_i(x) \in \mathbb{Z}[x], \deg(p_i) \leq 1$, $t(x) = \sum_{i=1}^{N} e_i p_i(x)^2$ は定数でない関数 $(\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z})$ とし,

$$\prod_{i=1}^{N} W_{E,P}(p_i(k))^{e_i}$$

の形の式の平方剰余が与えられているとすると, k の偶奇を $O(N\log^3 q)$ で計算できる.

証明 . 主結果 1 の式 (2) より, $n = p_1(k), \cdots, n = p_N(k)$ として掛け合わせることで,

$$\frac{\prod_{i=1}^{N}\phi(p_i(k))^{e_i}}{\prod_{i=1}^{N} W_{E,P}(p_i(k))^{e_i}} = \phi(P)^{t(k)}$$

を得る.

定理 3 より, $\phi(p_i(k))^{e_i}$, を N 個計算するのにかかる時間は $O(N\log^3 q)$ だから, 定理 2 と合わせて, 左辺を $O(N\log^3 q)$ で計算できる. 今, $\phi(P)$ は平方非剰余だから, $t(k)$ の偶奇は定数時間で計算できる. これらより, $t(0), t(1)$ を定数時間で計算することにより, k の偶奇を得られる. □

系 1. $P \in E_r$, $Q = kP$ $(0 \leq k < \mathrm{ord}(P))$ とする. また, $\phi(P)$ は平方非剰余であるとし, P, Q と, $W_{E,P}(k)$ の平方剰余を $O(T(q))$ で判定する方法が既知であるとする. このとき, k を $O(\log q(T(q) + \log^4 q))$ で計算できる.

証明 . 命題 3 で $N = 1, e_1 = 1, p_1(x) = x$ とし, k の偶奇を $O(T(q) + \log^3 q)$ で判定できることになる. これ

を命題 2 と合わせることによって

$$O((T(q)+\log^3 q)\log q+\log^4 q)=O(T(q)\log q+\log^4 q)$$

□

3 主結果の証明

まず, Section 1 に記述した主結果 1 を示す.

証明 . まず, 式 (2) が成り立つことを示す. 定理 1 より,

$$W_{E,aP}(n)\cdot W_{E,P}(a)^{n^2}=W_{E,P}(an)=W_{E,nP}(a)\cdot W_{E,P}(n)^{a^2}.$$

最左辺と最右辺を用いて,

$$\frac{W_{E,nP}(a)\cdot W_{E,P}(n)^{a^2}}{W_{E,P}(a)^{n^2}}=W_{E,aP}(n)$$

を得る. ここで, $a=q-1,q-1+r$ とすることで,

$$\frac{W_{E,nP}(q-1)\cdot W_{E,P}(n)^{(q-1)^2}}{W_{E,P}(q-1)^{n^2}}=W_{E,(q-1)P}(n),$$
$$\frac{W_{E,nP}(q-1+r)\cdot W_{E,P}(n)^{(q-1+r)^2}}{W_{E,P}(q-1+r)^{n^2}}=W_{E,(q-1+r)P}(n)=W_{E,(q-1)P}(n)$$

2 式より,

$$\frac{W_{E,nP}(q-1)\cdot W_{E,P}(n)^{(q-1)^2}}{W_{E,P}(q-1)^{n^2}}=\frac{W_{E,nP}(q-1+r)\cdot W_{E,P}(n)^{(q-1+r)^2}}{W_{E,P}(q-1+r)^{n^2}}$$

ゆえに,

$$\frac{W_{E,nP}(q-1)}{W_{E,nP}(q-1+r)}=\left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+r)}\right)^{n^2}\cdot W_{E,P}(n)^{2r(q-1)+r^2}$$

$2r(q-1)\equiv 0 \pmod{q-1}$ より, $W_{E,P}(n)^{2r(q-1)+r^2}=W_{E,P}(n)^{r^2}$ だから, 両辺を $\frac{1}{r^2}$ 乗して, 式 (2) を得る.
次に, $\phi(nP)$ が EDS であることを示す. 上式 (2) より,

$$\phi((m+n)P)\phi((m-n)P)\phi(P)^2=\phi(P)^{(m+n)^2+(m-n)^2+2}\cdot W_{E,P}(m+n)W_{E,P}(m-n),$$
$$\begin{aligned}&\phi((m+1)P)\phi((m-1)P)\phi(nP)^2-\phi((n+1)P)\phi((n-1)P)\phi(mP)^2\\&=\phi(P)^{(m+1)^2+(m-1)^2+2n^2}W_{E,P}(m+1)W_{E,P}(m-1)W_{E,P}(n)^2\\&\quad-\phi(P)^{(n+1)^2+(n-1)^2+2m^2}W_{E,P}(n+1)W_{E,P}(n-1)W_{E,P}(m)^2.\end{aligned}$$

上 2 式から, $\phi(nP)$ は EDS である. □

主結果 1 が示されたので, これにより定理 5 の証明が完了した.

次に, 主結果 2 を示す.

証明 . 問題 (2) ⇒ 問題 (1)

$P, Q = kP$ は既知だから, 楕円曲線上の加法により, $(k+1)P, (k+2)P$ を計算できる. 定理 5 より, $\phi(P)$ が $\mathbb{F}_q$ 上の原始根であれば, $\mathbb{F}_q$ 上の DLP に確率的に $O(\log^4 q)$ で帰着させることができる. $\mathbb{F}_q$ 上離散対数問題は確率的準指数時間で解けるため, k を得る.

問題 (1) ⇒ 問題 (2)

$0 < k \leq \mathrm{ord}(P)$ としてよい. 定理 2 より, $W_{E,P}(k)$ は $O(\log k \log^2 q) = O(\log^3 q)$ で計算することができる.

問題 (1) ⇒ 問題 (4)

定理 4 により, $Q = kP$ を $O(\log^4 q)$ で計算することができる.

問題 (4) ⇒ 問題 (1)

$P, Q = kP$:既知だから, 楕円曲線上の加法により, $(k+1)P, (k+2)P$ を計算できる. 定理 3 より, $\phi(Q), \phi((k+1)P), \phi((k+2)P)$ を $O(\log^3 q)$ で計算できる.

問題 (6) ⇒ 問題 (5)

主結果 1 の式 (1) で, $n = ab$ とすると,

$$\phi(abP) = \frac{1}{\phi(P)} \left(\frac{W_{E,abP}(q-1)}{W_{E,abP}(q-1+r)} \right)^{\frac{1}{r^2}} \tag{1}$$

上式の右辺の括弧内の計算は, 定理 2 より, $O(\log^3 q)$ で計算できる.

問題 (5) ⇒ 問題 (6)

補題 1 の式 (6) で, $n = ab$ として,

$$\frac{\phi((ab-1)P)\phi((ab+1)P)}{\phi((ab)^2)P} = \phi(P)^2 \left(x(P) - x(abP) \right). \tag{2}$$

今, 問題 5 が解けるという仮定のもと, $\phi(abP)$ は計算できる. $\phi(nP)$ は EDS であるから,

$$\phi((m+n)P)\phi((m-n)P)\phi(P)^2 = \phi((m+1)P)\phi((m-1)P)\phi(nP)^2 - \phi((n+1)P)\phi((n-1)P)\phi(mP)^2$$

が成り立つ. ここで, $m = ab, n = b$ とすると,

$$\phi((a(b+1))P)\phi(a(b-1)P)\phi(P)^2 = \phi((ab+1)P)\phi((ab-1)P)\phi(aP)^2 - \phi((a+1)P)\phi((a-1)P)\phi(abP)^2.$$

P, aP, bP が既知なので, 楕円曲線上の加法により, $(a+1)P, (a-1)P, (b+1)P, (b-1)P$ は計算できる. よって, 問題 5 が解けるという仮定から, $\phi((ab+1)P)\phi((ab-1)P)$ を, それ以外の部分を計算することによって求めることができる. これと上式より, $x(abP)$ を計算できる. 楕円曲線の式に代入して計算することで, 対応する abP の候補を 2 つ得ることができる. 定理 3 より, $O(\log^3 q)$ で $\phi(abP)$ を計算し, 問題 5 を解いて得られる $\phi(abP)$ と比較することで, 2 つのうち正しい abP を決定できる.

問題 (1) ⇒ 問題 (5) aP, bP が既知のとき, 問題 1 を解いて a, b をそれぞれ計算できるので, P から abP を計算することができる.

問題 (3) ⇒ 問題 (1)

系 1 より, 問題 3 が $O(T(q))$ で解けるとすると, $O((\log q)(T(q) + (\log q)^4))$ で問題 1 を計算することができる.

問題 (2) ⇒ 問題 (3)

[1] の Algorithm 2.3 により, この平方剰余判定は $O(\log^3 q)$ で確率的に計算できる. □

4 まとめ

本論文では, r を固定し, 楕円曲線上の点 P を r-ねじれ点から選ぶことで, 先行研究でなされている結果を, $\mathrm{ord}(P)$ が素数でない場合まで拡張することを考えた. 結果, $r > 3, \gcd(r, q-1) = 1$ としてある程度 r に条件をつけ, 写像 ϕ を定義することによって, 先行研究と同様の結果を得ることができた.

今後の課題として考えられることは, elliptic net 上のものを含むここで扱っていないほかの計算困難問題との関係性を加えることや, 主結果 2 において, $\phi(P)$ を原始根とした条件などをより緩和することなどが挙げられる.

5 謝辞

本研究は, 著者が首都大学東京大学院理学研究科数理科学専攻博士前期課程在学中に, 同大学院理学研究科数理科学専攻の内田幸寛准教授のご指導の下におこなったものである. 適切な助言と, 熱心な指導をしてくださった内田幸寛准教授に深く感謝いたします. また, ご多忙の中において, 本論文の副査を快く引き受けてくださいました内山成憲教授と横山俊一准教授にも深く感謝いたします. 学部 4 年次から 3 年間, 同じ研究室の仲間として苦楽を共にした石川岳氏と梶野智哉氏, そしてこれまで支えてきてくださった家族の皆様にも, 心よりお礼申し上げます. 本当にありがとうございました.

参考文献

[1] Bach, E.(1990). A Note on Square Roots in Finite Fields. IEEE trasactions on information theory. vol.36, no.6, 1494–1498.

[2] Bach, E., Shallit, J.(1996). Algorithmic number theory, Efficient algorithms. Foundations of Computing Series, vol.1. MIT Press, Cambridge.

[3] Fong, K., Hankerson, D., LopezJ., Menezes, A.(2003). Field inversion and point halving revisited. technical Report. CORR 2003-18, Department of Combinatorics and Optimization, University of Waterloo, Canada.

[4] Lauter, K.E., Stange, K.E.(2008). The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences, in: Proc. of SAC 2008, LNCS-5381, 309–327, Springer-Verlag, Berlin.

[5] Shipsey, R.(2001). Elliptic Divisibility Sequences. PhD thesis, Goldsmiths, University of London.

[6] Shipsey, R., Swart, C.(2008). Elliptic divisibility sequences and the elliptic curve discrete logarithm problem, http://eprint.iacr.org/2008/444 .

[7] Stange, K.E.(2008). Elliptic nets and elliptic curves. PhD thesis, Brown University.

[8] Ward, M.(1948). Memoir on elliptic divisibility sequences. American Journal of Mathmatics. vol.70, 1, 31–74.

[9] Washington, L.C.(2008). Elliptic Curves : Number Theory and Cryptography(Second Edition). Chapman and Hall/CRC.

[10] Yarimizu, J., Uchida, Y., Uchiyama, S.(2014). The elliptic curve Diffie-Hellman problem and an equivalent hard problem for elliptic divisibility sequences. JSIAM Letters Vol.6, 5–7.